10/[illegible]5743

PCT / SE 2004 / 0 0 1 1 3 1

PRV
PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

REGISTRERINGSVERKET • PAT

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* / *Applicant (s)* — *Dan Duroj, Bandhagen SE*

(21) *Patentansökningsnummer* / *Patent application number* — *0302189-6*

(86) *Ingivningsdatum* / *Date of filing* — *2003-08-11*

Stockholm, 2004-07-21

För Patent- och registreringsverket
For the Patent- and Registration Office

Anita Södervall

Anita Södervall

Avgift
Fee

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

Tekniskt område

Föreliggande uppfinning anger en handhållen nätverksanslutning skapad med åtminstone två lagringsmedium i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks åtkomstblockering i form av åtminstone ett av en brandvägg, SOCKS, IP-filter, eller proxy. Uppfinningen anger även ett förfarande för detsamma.

Teknikens ståndpunkt

Frånvaron av en enkel plattform för distributionshantering och nätverkskommunikation samt datalagring för den ordinärt kunniga datoranvändaren är en bromsande faktor i IT-samhället i dag. IT-kommissionen fastslår att det är för svårt att använda Internet och på grund av det kommer det att finnas två klasser i samhället, de som har utbildning att använda Internet och de som inte har det. Företag och privatpersoner skickar och lagrar, samt arbetar med allt större filer över nätverk. För att klara detta används programvaror som Email, FTP, Http-baserade webbgränssnitt samt VPN-lösningar.

En rad problem uppkommer för den ordinäre datoranvändaren. Alla PC-baserade datorer går förr eller senare sönder, vilket leder till att både personliga värden och företagsvärden går förlorade med följd att exempelvis backup saknas och är tom. Datalagring i hemmet och på arbetsplatser är av olika anledningar utsatt för insyn och åtkomst av obehöriga, vilket leder till efterfrågan på krypterad säker datalagring. Anställda samt privatpersoner vill från och till distribuera filer i storlekar upp till 1GB. Detta är i praktiken omöjligt för en person utan IT-utbildning att klara detta, vilket leder till att data skickas med hjälp av CD skivor, disketter, Pocketminnen mm.

Förmågan att kunna flyta runt mellan olika arbetsgrupper, företag, samt hem och fritid och alltid komma åt sina filer är en av de starkaste drivkrafterna för Internet relaterad verksamhet. I princip är denna möjlighet alltid avstängd, då företag reglerar åtkomst och rädslan för intrång med hjälp av att stänga ner portar i brandväggar, proxys, och IP-filter. Detta leder till att enbart publika kanaler finns tillgängliga för företaget såsom http och Email, Newsgroups eller liknande. Det är en utveckling som medför att filer skickas med http i stället för FTP, och där fler och fler tjänster tvingas att försöka att leva i HTML-form över publika bläddrare (browser) när de i själva verket är av privat natur, dvs. företag till företag, person till person, anbud och accept förfaranden.

Det existerar konkurrerande system såsom Email. En email-administratör delar normalt inte ut mer än 2 till 5 MB per konto. Om mer utrymme önskas börjar det kosta betydligt mer pengar. Dagens email-klienter laddar hem informationen vid uppkoppling, vilket medför att på

platser med låg bandbredd kommer ett större mail att göra email åtkomst obrukbar för en längre eller kortare tid.

FTP är av tradition ett verktyg för den utbildade nätverksadministratören och kräver:

1. Djupare kunskaper om nätverk
2. Kännedom om IP-adressen/namnadressen
3. Programvara installerad både på egen dator och hos den som motar filer.

Http-baserade webbgränssnitt som hämtas från exempelvis projektplatsen.se HOME SE Xdrive.com medför att:

1. Programvaran måste installeras på egen dator
2. Programvara körs genom vanliga kommersiella webbläsare
3. Säkerheten blir inte större än vid vanlig publik webbläsning dvs Explorer Netscape 128 bitars kryptering
4. Det är krångligt att dela filer med andra
5. Dokument kan inte redigeras direkt i gränssnittet
6. Reklam mottas från webbläsaren , reklam relaterade "cookies", Active X, JavaScript-program mm installeras utan vetskap på egen dator

Så kallad "Peer-to-Peer" kommunikation är en modell som bygger på att den anonyme användaren är villig att distribuera filer samt upplåta en del av sin egen dator till okända användare i ett anonymt nätverk.

Problem med Virtual Private Network (VPN) uppkommer då det:

1. Kräver installation med begränsat antal användare till fasta datorer
2. Det går att ladda ned över ett webbgränssnitt men blir då olidligt långsamt och klumpigt
3. Att arbeta mobilt kräver att användaren måste bära med dig den dator som programvaran är installerad på samt, att de företag eller det nätverk arbete sker i tillåter dig att koppla in egen dator i den miljön.

HDD på USB och HDD på PCMCIA medför problem i det att filer ligger på kortet/nyckeln, inte på en server. Förloras kortet/nyckeln förloras filerna.

Sammanfattning av uppfinningen

För att lösa problem som nämnts ovan och andra liknande anger föreliggande uppfinning en handhållen nätverksanslutning skapad med åtminstone två lagringsmedium i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks åtkomstblockering i form av åtminstone ett av en brandvägg, SOCKS, IP-filter, eller proxy. Härvid har varje lagringsmedium ett gränssnitt mot en värddator i nätverken och via programvaran upprättas en kommunikation med värddatorn inuti företagsnätverket genom att låna värddatorns temporära kataloger, vilket ger åtkomst till värddatorn utan att störa värddatorns filstruktur.

En krypto-daemon ingår, vilken innefattar en uppkopplingsmetodik som prövar att upprätta en tunnling genom åtkomstblockeringen mot en central extern server avseende typ av tillåtna datapaket för kommunikation mot existerande typ av åtkomstblockering, varvid krypto-daemon upprättar tunnlingen mot den externa centrala servern genom åtkomstblockeringen via en provupprättning av en kommunikation med åtkomstblockeringen. Uppkopplingsmetodiken anpassar sig till efterfrågad typ av datapaket genom att repetitivt fråga åtkomstblockeringen efter tillåten typ av datapaket ända till dess att rätt typ påträffas genom att minnas och repetitivt utelämna felaktiga förfrågningar, och genom att vid rätt fråga förändra datapakets datastruktur till efterfrågad struktur för den specifika port som står tillbuds för kommunikationen.

Härvid upprättas ett externt nätverk via den externa centrala servern belägen utanför nätverken för samtidig kommunikation genom åtminstone två lagringsmedium och dess programvara, varvid tunnling genom åtkomstblockeringen har åstadkommits utan att göra intrång i nätverket i sig, medförande mot åtkomstblockeringen fri kapacitet för kommunikation med datapaket.

En utföringsform av metodiken anges av följande pseudokod vid uppkoppling mot önskad port:

```
Kolla om proxy skall användas
Om "OK"
  Prova HTTP-proxy
```

```
Om "OK"
 Koppla upp via HTTP-proxy
Annars
 Prova SOCKS4-proxy
 Om "OK"
  Koppla upp via SOCKS4-proxy
 Annars
  Prova SOCKS5-proxy
  Om "OK"
   Koppla upp via SOCKS5-proxy
  Annars
   Prova direktuppkoppling
   Om "OK"
    Gör direktuppkoppling
   Annars
    Uppkoppling misslyckades eller prova annan port.
Annars
 Prova direktuppkoppling
 Om "OK"
  Gör direktuppkoppling
 Annars
  Uppkoppling misslyckades eller prova annan port.
```

En ytterligare utföringsform av metodiken innefattar för en framtida generation av proxy/brandväggar som endast släpper igenom "godkänd" trafik, att detta kringgås genom att gömma skickat data genom att sända över en fejkad HTML-sida med datat maskat.

I en utföringsform är filer åtkomstbara via värddatorn, vilka hämtas och krypteras i värddatorns temporära katalog, varvid de läggs ut krypterade på den externa centrala servern med bestämd åtkomstprofil som medger åtminstone läsning av filen men inte kopiering från dator utanför nätverket med ansluten värddator, vilket medger display av filer utanför nätverket.

En annan utföringsform medger att mediets användare kan röra sig i ett främmande nätverk och kommunicera externt via den externa centrala servern med andra användare av mediet via tunnlingen.

En utföringsform inkluderar att mediets programvara innefattar IP-telefoni, varvid användare av mediet från valfri datoriserad anordning i valfritt nätverk kan upprätta spontan mobil IP-telefoni via den centrala servern.

Ytterligare en utföringsform innefattar att skapa åtminstone ett av en radiokanal och filmkanal med andra användare i det externa nätverket genom att mediets programvara innefattar "streaming" media, varvid användarna kan konsumera musik och film.

En ytterligare utföringsform inkluderar att mediets programvara innefattar versionshantering, vilket medför att tidigare versioner av filer kan återskapas genom att spara undan förändringar i ett separat minne i den centrala externa servern som kopplas på/av genom en omkopplare för detsamma på begäran av en användare.

Ännu en utföringsform innefattar att mediets programvara medger flera användare av detsamma att bearbeta en gemensam textfil i realtid genom den centrala externa servern.

Vidare avser föreliggande uppfinning ett förfarande för en handhållen nätverksanslutning skapad med åtminstone två lagringsmedium i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks åtkomstblockering i form av åtminstone ett av en brandvägg, SOCKS, IP-filter, eller proxy. Uppfinningen enligt förfarandet innefattar stegen:

att varje lagringsmedium har ett gränssnitt mot en värddator i nätverken och via programvaran upprättar kommunikation med värddatorn inuti företagsnätverket genom att låna värddatorns temporära kataloger, vilket ger åtkomst till värddatorn utan att störa värddatorns filstruktur;

en uppkopplingsmetodik som innefattad i en krypto-daemon som prövar att upprätta en tunnling genom åtkomstblockeringen mot en central extern server avseende typ av tillåtna datapaket för kommunikation mot existerande typ av åtkomstblockering, varvid nämnda krypto-daemon upprättar tunnlingen mot centralservern genom åtkomstblockeringen via en provupprättning av en kommunikation med åtkomstblockeringen, varvid uppkopplingsmetodiken anpassar sig till efterfrågad typ av datapaket genom att repetitivt fråga åtkomstblockeringen efter tillåten typ av datapaket ända till dess att rätt typ påträffas genom att minnas och repetitivt utelämna felaktiga förfrågningar, och genom att vid rätt fråga förändra datapakets datastruktur till efterfrågad struktur för den specifika port som står tillbuds för kommunikationen; och

varvid ett externt nätverk upprättas via den externa centrala servern belägen utanför nätverken för samtidig kommunikation genom åtminstone två lagringsmedium och

dess programvara, varvid tunnling genom åtkomstblockeringen har åstadkommits utan att göra intrång i nätverket i sig, medförande mot åtkomstblockeringen fri kapacitet för kommunikation med datapaket.

Ytterligare förfarandekrav definieras av de anslutna osjälvständiga förfarandepatentkraven som vad avser innehållet har sin motsvarighet i utföringsformerna enligt anordningskraven.

Kortfattad beskrivning av ritningarna

I den löpande texten hänvisas nu till bilagda ritningsfigurer för en bättre förståelse av uppfinningen och dess utföringsformer, varvid:

Fig. 1 schematiskt visar hur en kommunikation upprättas mellan företagsnätverk enligt teknikens ståndpunkt,

Fig. 2 schematiskt visar hur en nätverksanslutning åstadkoms via tunnling enligt föreliggande uppfinning.

Detaljerad beskrivning av föredragna utföringsformer

I fig. 1 beskrivs schematiskt hur en kommunikation upprättas mellan företagsnätverk 10, 12, 14 enligt teknikens ståndpunkt. Anslutna till nätverken, LAN eller liknande, är lokala datorer 16. Den streckade linjen mellan lokala datorer anger att fler än två datorer 16 kan vara anslutna till nätverken 10, 12, 14. Nätverken 10, 12, 14 styrs via nätverksservrar 18 i respektive nätverk. För att upprätta en kommunikation mellan exempelvis datorer 16 i nätverken 10, 12, 14 måste nätverkens åtkomstskydd/-blockering för extern trafik forceras. Åtkomstskyddet utgörs vanligtvis av en eller flera av brandvägg, SOCKS, IP-filter, eller proxy, här, i utföringsformen enligt fig. 1 exemplifieras med en brandvägg (FW, 20).

I exemplet enligt fig. 1 initieras en paketdatakommunikation via Internet 22 från en dator 16 i nätverket 10 respektive en dator 16 i nätverket 12, prickad linje i fig. 1. Likaledes öppnas en kommunikation mellan en andra dator 16 i nätverket 10 mellan en dator 16 i nätverket 14, vilket är markerat med en streckad linje i fig. 1. För att kommunicera mellan datorerna 16 måste brandväggarna 20 i respektive nät 10, 12, 14 forceras. Datorerna 16 använder naturligtvis avsett protokoll för forcering av brandväggarna, varvid datahuvuden i paket som sänds i kommunikationen är rätt inställda för detta ändamål. Varje nätverk 10, 12, 14 har dock egna restriktioner satta för en upprättad kommunikation i form av vilka filer, hur mycket data mm som får sändas och mottas, vilket regleras via brandväggen 20.

Speciellt är det av datasekretesskäl ytterst svårt att forcera en brandvägg 20 utifrån och in i ett nätverk 10,12, 14, även med legal information i datapaketen pga satta restriktioner i

brandväggar 20. Därför är det svårt att kommunicera mellan nätverk 10, 12, 14 och dess datorer 16. Exempelvis kan en anställd i något av företagen med nätverken 10, 12, 14 inte tillfullo utföra relevant arbete från sin hem-PC mot nätverken 10, 12, 14 med de restriktioner för utifrån kommande trafik som kontrolleras av brandväggarna 20. Andra exempel på restriktioner, problem och svårigheter för en enkel mångsidig datakommunikation från och till nätverk 10, 12, 14 via brandvägg, SOCKS, IP-filter, eller proxy har nämnts ovan i föreliggande uppfinnings problemställning och upprepas inte specifikt här, utan är välkända för en fackman inom teknikområdet.

I fig. 2 visas schematiskt hur en nätverksanslutning åstadkoms via tunnling enligt föreliggande uppfinning. Visade organ i fig. 1 som överensstämmer med de i fig. 2 har försetts med likadana hänvisningsbeteckningar. För att åstadkomma nätverksanslutningen enligt föreliggande uppfinning används ett i och för sig förut känt lagringsmedium 24, 26, 28 i form av vilken som helst anordning som är bärbar, företrädesvis i fickformat, med elektroniskt minne för lagring av programvara och ett gränssnitt mot en dator för upprättning av en tunnling via en dator 16 genom en brandvägg, SOCKS, IP-filter, eller proxy. Fortsättningsvis används en brandvägg 20 för att exemplifiera uppfinningen, men fackmannen förstår att även andra åtkomstskydd kan forceras med konceptet enligt föreliggande uppfinning, varvid dessa härmed innefattas i enlighet med bilagda patentkravs avfattning. Detsamma gäller för lagringsmediet, viket här exemplifieras som ett i form och storlek av ett kreditkort med en mini-CD-lagringsyta för innefattad programvara. Andra lagringsmedium som kan användas enligt föreliggande uppfinning utgörs av exempelvis mobiltelefon, personlig digital assistent (PDA) och andra för fackmannen kända anordningar. Gränssnittet mot dator 16 utgörs av en CD-kortsläsare -släde vad beträffar mini-CD kortet 24, 26, 28, och kabel eller trådlös överföring mellan datorer vad avser mobiltelefon och PDA på för fackmannen känt vis.

Lagringsmediet innefattar enligt en utföringsform av uppfinningen ett grafiskt gränssnitt med drag & drop-funktionalitet, automatisk uppkoppling utan att användaren behöver känna till eller hantera IP-adressering. Lagringsmediet 24, 26, 28 har en klientserver-mjukvara där klienten ligger på mediet 24, 26, 28, varvid mediet i en utföringsform som kort i kreditkortsstorlek har en mini-CD-skiva inpräglad utgörs av en FlexDisc-CD ®. Kortet med CD-skivan fungerar som en nyckel och läggs i en dators 29 CD-släde. Programvaran på CD-skivan medger en användare att arbeta transparent genom brandväggar och Proxy med föreliggande uppfinning. Föreliggande uppfinning lämnar inga spår på de datorer som används för upprättande av en nätverksanslutning.

Fakta avseende mini-CD-kortet i en utföringsform:

- Enkel fildelning utan webbläsare
- 2048 bitars kryptering
- Automatisk filsynkronisering
- Företagsfolder (intranet)
- Unikt lösenordsskyddad nätverksfolder (extranet)
- Brandväggsvänlig kommunikation med endast 1 port, tunnling över HTTPS sockets
- Egen inbox, tar emot filer via email
- Mailar filer via SSL-länkar
- Stöder portabel CD-media-användning
- Multi-fönster för flera aktiva konton

För att utöva föreliggande uppfinning används en handhållen nätverksanslutning skapad med åtminstone två lagringsmedium 24, 26, 28 i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks 10, 12, 14 åtkomstblockering i form av en brandvägg 20. Varje lagringsmedium 24, 26, 28 har ett gränssnitt här CD-släde för mini-CD-kort, mot en värddator 29 i nätverken 10, 12, 14. Via programvaran på kortet 24, 26, 28 upprättas en kommunikation med värddatorn 29 inuti företagsnätverket 10, 12, 14 genom att låna värddatorns 29 temporära kataloger, vilket ger åtkomst till värddatorn 29 utan att störa värddatorns filstruktur.

För att åstadkomma sagda används en krypto-daemon (programvara) som innefattar en uppkopplingsmetodik som prövar att upprätta en tunnling genom åtkomstblockeringen 20 mot en central extern server 30 avseende typ av tillåtna datapaket för kommunikation mot existerande typ av åtkomstblockering 20. Krypto-daemon upprättar tunnlingen 32, här schematiskt visat som rörformad genom brandväggen 20 i fig. 2, mot den centrala externt, för nätverken 10, 12, 14, belägna servern 30, genom åtkomstblockeringen 20 via en provupprättning av en kommunikation med åtkomstblockeringen 20. Den tunnlade 32 kommunikationen i fig. 2 anges med streckade linjer och i den externa centrala servern 32 har en cirkelformad minnesarea schematiskt angetts som en knutpunkt för kommunikation mellan användare av lagringsmedium 24, 26, 28. Minnesarean är inte begränsad i storlek och här kan skilda innehavare av lagringsmedium 24, 26, 28 ha konto för fillagring och andra transaktioner mellan medium 24, 26, 28.

Servern 30 enligt en utföringsform av föreliggande uppfinning har bl a följande egenskaper:
- skrivet i ANSI C/C++
- Stöd för Quota

- kan dela ut UNIX/Windows/HFS+ filsystem
- LINUX/Solaris/BSD-kompatibel
- Minimerar nätverksbelastning
- Skydd mot hackerangrepp, minimal exponering mot nätverket.

Vidare har mediet 24,26,28 följande klientegenskaper:

- 32bit Windows-program
- Win95/98/ME/2000/NT/XP-kompatibel
- Ingen installation
- Konfigurerbart användargränssnitt
- Drag & drop
- Autostart
- stöd för alla filformat
- Enbart utgående trafik från klienten

Uppkopplingsmetodiken anpassar sig till efterfrågad typ av datapaket genom att repetitivt fråga åtkomstblockeringen efter tillåten typ av datapaket. Detta sker till dess att rätt typ påträffas genom att metodiken minns och repetitivt utelämnar felaktiga förfrågningar, och genom att vid rätt fråga förändra datapakets datastruktur till efterfrågad struktur för den specifika port som står tillbuds för en kommunikation.

Med metodiken i daemon upprättas ett externt nätverk via den externa centrala servern 30 belägen utanför nätverken 10, 12, 14 för samtidig kommunikation genom åtminstone två lagringsmedium 24, 26, 28 och dess programvara. Härvid åstadkoms tunnling 32 genom åtkomstblockeringen 20, utan att göra intrång i nätverket 10, 12, 14 i sig, medförande mot åtkomstblockeringen 20 fri kapacitet för kommunikation med datapaket.

<u>Uppkopplingsmetodik</u>

Här ges nu ett exempel på en möjlig utföringsform av en uppkopplingsmetodik enligt föreliggande uppfinning. Portar som *kan* vara öppna genom proxy/brandväggar utgörs av:

FTP (21)
SSH (22)
Telnet (23)
SMTP (25) (utgående mail)
HTTP (80)
POP3 (110) (inkommande mail)
HTTPS (443)

Det finns fler portar, men dessa är de som är mest troliga. Av dessa är port 80 och 443 med största sannolikhet öppna genom brandväggar exempelvis för att möjliggöra surfning på nätet. Däremot är det många proxy som bara godkänner trafik mot port 443. I metodiken enligt föreliggande utföringsform används port 443, dels pga ovanstående, och dels pga att data som skickas där förväntas vara krypterat.

Tillvägagångssätt anges här som pseudokod vid uppkoppling mot port 443:

```
Kolla om proxy skall användas
Om "OK"
 Prova HTTP-proxy
 Om "OK"
  Koppla upp via HTTP-proxy
 Annars
  Prova SOCKS4-proxy
  Om "OK"
   Koppla upp via SOCKS4-proxy
  Annars
   Prova SOCKS5-proxy
   Om "OK"
    Koppla upp via SOCKS5-proxy
   Annars
    Prova direktuppkoppling
    Om "OK"
     Gör direktuppkoppling
    Annars
     Uppkoppling misslyckades eller prova annan port
Annars
 Prova direktuppkoppling
 Om "OK"
  Gör direktuppkoppling
 Annars
  Uppkoppling misslyckades eller prova annan port
```

Ytterligare innefattad i metodiken, i en framtid, om kommande generation av proxy/brandväggar bara släpper igenom "godkänd" trafik, t.ex. HTML-kod så kan den

kringgås genom att gömma skickat data genom att sända över en fejkad HTML-sida med datat maskat som en bild eller liknande. Ytterligare ett alternativ i en metodik är att prova uppkoppling via andra portar än 443 om denna skulle misslyckas.

Föreliggande uppfinning möjliggör att filer nås via värddatorn 29 hämtas och krypteras i värddatorns 29 temporära katalog. Där läggs de ut krypterade på den externa centrala servern 30 med bestämd åtkomstprofil som medger åtminstone läsning av filen men inte kopiering från dator utanför nätverket med ansluten värddator 29, vilket medger display/visning av filer utanför nätverket.

Mediet 24, 26, 28 medger dess användare att röra sig i ett främmande nätverk 10, 12, 14 och kommunicera externt via den externa centrala servern 30 med andra användare av mediet via tunnlingen 32. Vidare så innefattar mediets 24, 26, 28 programvara IP-telefoni i en utföringsform, varvid användare av mediet från valfri datoriserad 16, 29 anordning i valfritt nätverk 10, 12, 14 kan upprätta spontan mobil IP-telefoni via den externa centrala servern 30.

Föreliggande uppfinning gör det möjligt att skapa åtminstone ett av en radiokanal och filmkanal med andra användare i det externa nätverket genom att mediets 24, 26, 28 programvara innefattar streaming media, varvid användarna kan konsumera musik och film via tunnling 32.

En ytterligare fördelaktig utföringsform åstadkommer att mediets programvara innefattar versionshantering, vilket medför att tidigare versioner av filer kan återskapas genom att spara undan förändringar i ett separat minne i den centrala externa servern 30 som kopplas på/av genom en omkopplare på begäran av en användare.

Vidare kan mediets 24, 26, 28 programvara i en utföringsform anpassas att medge flera användare av mediet 24, 26, 28 att bearbeta en gemensam textfil i realtid genom den centrala externa servern 30.

Föreliggande uppfinning löser både en enskild medarbetares och ett företags behov av omedelbar backup, åtkomst av gemensam och privat arbetsyta samt uppbyggnad av effektiva nätverk med nya kunder, företag eller inhyrda konsulter. Den fungerar/verkar omgående i befintlig infrastruktur.

Den enkla mobiliteten, möjligheten att arbeta på vilken dator som helst medför förmodligen att allt fler väljer att bära med sig lagringsmedium som används enligt föreliggande

uppfinning istället för tunga laptop-datorer. Slitage och kostnader för bärbara maskiner minskar. Trycket på systemadministratören minskar, eftersom denne kan dela ut kort till nyanställda, konsulter, kunder och medarbetare som omgående behöver arbetsyta, intranät, extranet, samt email. Lagringsmediet är ett gruppverktyg som kan delas ut på ett möte utan förberedelser och där alla inblandade får tillgång till en gemensam arbetsyta samt en egen arbetsyta med egen email box

Risken att obehöriga stjäl information från ett företag minskar när föreliggande uppfinning används Det är säkert att handha filer i enlighet med föreliggande uppfinning endast lösenord och användarnamn behöver memoreras.

Föreliggande uppfinning gör det möjligt, för kontorspersonal, receptionister, som är satta att skicka och ta emot stora filer på Internet åt ett företag och des anställda, att klara denna uppgift, med den dator de har tillgång till. De behöver inte längre skicka data med CD, syquest, disketter, bärbara hårddiskar, med post, bud ,taxi osv. Den kostnaden är borta.

Uppfinningen enligt föreliggande koncept möjliggör att företag har råd att sprida ut lagringsmedium till dem som behöver det utan att överväga kostnaden per VPN-licens eller att anlita en systemadministratör för att installera krångliga licenser. Beroendet av komplexa och dyra mjukvarusystem för "groupware"-användande försvinner. Vidare medger uppfinningen att alla på ett företag erhåller en enkel backup. Vid förlust av data på företaget kan den anställde ta hem de förlorade filerna från sitt konto och ingen tid har förlorats. Om datorerna i företaget har blivit stulna eller förstörda kan den anställde omgående arbeta på vilken som helst dator med Internetuppkoppling som finns tillhands. Företagets personal behöver inte längre sitta och vänta på hjälp av systemadministratören för att klara av att dela filer i ett nytt projekt.

Enkelheten i lösningen och den låga kostnaden per klient gör föreliggande uppfinning till ett effektivt verktyg att bygga en infrastruktur för ett företag eller organisation. En säljare i ett företag, som använder, föreliggande uppfinning kan komma till ett främmande företag och omedelbart arbeta på vilken som helst PC i den okända miljöns infrastruktur.

Förmågan att kunna flyta runt mellan olika arbetsgrupper, företag, hem, fritid och att alltid komma åt nätverket skapar trygghet för en säljare, privatperson etc., som ska ut på resa eller på annat sätt förflytta sig mellan olika platser. "Skräcken" att ha glömt filerna på kontoret vid resa minskar med föreliggande uppfinningskoncept.

Patentkrav

1. Handhållen nätverksanslutning skapad med åtminstone två lagringsmedium (24, 26, 28) i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks (10, 12, 14) åtkomstblockering i form av åtminstone ett av en brandvägg (20), SOCKS, IP-filter, eller proxy, **kännetecknad** av att:

varje lagringsmedium (24, 26, 28) har ett gränssnitt mot en värddator (29) i nätverken (10, 12, 14) och som via programvaran upprättar kommunikation med värddatorn (29) inuti nätverket (10, 12, 14) genom att låna värddatorns (29) temporära kataloger, vilket ger åtkomst till värddatorn (29) utan att störa värddatorns filstruktur;

en krypto-daemon som innefattar en uppkopplingsmetodik som prövar att upprätta en tunnling (32) genom åtkomstblockeringen mot en central extern server (30) avseende typ av tillåtna datapaket för kommunikation mot existerande typ av åtkomstblockering, varvid nämnda krypto-daemon upprättar tunnlingen (32) mot den externa centrala servern (30) genom åtkomstblockeringen via en provupprättning av en kommunikation med åtkomstblockeringen, varvid uppkopplingsmetodiken anpassar sig till efterfrågad typ av datapaket genom att repetitivt fråga åtkomstblockeringen efter tillåten typ av datapaket ända till dess att rätt typ påträffas genom att minnas och repetitivt utelämna felaktiga förfrågningar, och genom att vid rätt fråga förändra datapakets datastruktur till efterfrågad struktur för den specifika port som står tillbuds för kommunikationen; och

varvid ett externt nätverk upprättas via den externa centrala servern (30) belägen utanför nätverken för samtidig kommunikation genom åtminstone två lagringsmedium (24, 26, 28) och dess programvara, varvid tunnling (32) genom åtkomstblockeringen har åstadkommits utan att göra intrång i nätverket (10,12, 14) i sig, medförande mot åtkomstblockeringen fri kapacitet för kommunikation med datapaket.

2. Nätverksanslutning enligt krav 1, **kännetecknad** av att metodiken anges av följande pseudokod vid uppkoppling mot önskad port:

```
Kolla om proxy skall användas
Om "OK"
  Prova HTTP-proxy
  Om "OK"
    Koppla upp via HTTP-proxy
  Annars
    Prova SOCKS4-proxy
    Om "OK"
```

Koppla upp via SOCKS4-proxy
Annars
Prova SOCKS5-proxy
Om "OK"
Koppla upp via SOCKS5-proxy
Annars
Prova direktuppkoppling
Om "OK"
Gör direktuppkoppling
Annars
Uppkoppling misslyckades eller prova ny port.
Annars
Prova direktuppkoppling
Om "OK"
Gör direktuppkoppling
Annars
Uppkoppling misslyckades eller prova ny port.

3. Nätverksanslutning enligt krav 1, **kännetecknad** av att metodiken innefattar för en framtida generation av proxy/brandväggar (20) som endast släpper igenom "godkänd" trafik, att detta kringgås genom att gömma skickat data genom att sända över en fejkad HTML-sida med datat maskat.

4. Nätverksanslutning enligt krav 1-3, **kännetecknad** av att filer åtkomstbara via värddatorn (29) hämtas och krypteras i värddatorns temporära katalog, varvid de läggs ut krypterade på den externa centrala servern (30) med bestämd åtkomstprofil som medger åtminstone läsning av filen men inte kopiering från en dator utanför nätverket (10, 12, 14) med ansluten värddator (29), vilket medger display av filer utanför nätverket (10, 12, 14).

5. Nätverksanslutning enligt krav 1-4, **kännetecknad** av att mediet (24, 26, 28) medger dess användare att röra sig i ett främmande nätverk (10, 12, 14) och kommunicera externt via den externa centrala servern (30) med andra användare av mediet (24, 26, 28) via tunnlingen (32).

6. Nätverksanslutning enligt krav 1-5, **kännetecknad** av att mediets (24, 26, 28) programvara innefattar IP-telefoni, varvid användare av mediet från valfri datoriserad

anordning (16, 29) i valfritt nätverk (10, 12, 14) kan upprätta spontan mobil IP-telefoni via den centrala servern (30).

7. Nätverksanslutning enligt krav 1-6, **kännetecknad** av att skapa åtminstone ett av en radiokanal och filmkanal med andra användare i det externa nätverket genom att mediets (24, 26 28) programvara innefattar streaming media, varvid användarna kan konsumera musik och film.

8. Nätverksanslutning enligt krav 1-7, **kännetecknad** av att mediets (24, 26 28) programvara innefattar versionshantering, vilket medför att tidigare versioner av filer kan återskapas genom att spara undan förändringar i ett separat minne i den centrala externa servern (30) som kopplas på/av genom en omkopplare för detsamma på begäran av en användare.

9. Nätverksanslutning enligt krav 1-8, **kännetecknad** av att mediets (24, 26, 28) programvara medger flera användare av detsamma att bearbeta en gemensam textfil i realtid genom den centrala externa servern (30).

10. Förfarande för en handhållen nätverksanslutning skapad med åtminstone två lagringsmedium (24, 26, 29) i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks åtkomstblockering i form av åtminstone ett av en brandvägg (20), SOCKS, IP-filter, eller proxy, **kännetecknat** av stegen:

att varje lagringsmedium (24, 26, 29) har ett gränssnitt mot en värddator (29) i nätverken (10, 12, 14) och via programvaran upprättar kommunikation med värddatorn (29) inuti nätverket (10, 12, 14) genom att låna värddatorns (29) temporära kataloger, vilket ger åtkomst till värddatorn (29) utan att störa värddatorns filstruktur;

en uppkopplingsmetodik som är innefattad i en krypto-daemon som prövar att upprätta en tunnling (32) genom åtkomstblockeringen mot en central extern server (30) avseende typ av tillåtna datapaket för kommunikation mot existerande typ av åtkomstblockering, varvid nämnda krypto-daemon upprättar tunnlingen mot den centrala servern (30) genom åtkomstblockeringen via en provupprättning av en kommunikation med åtkomstblockeringen, varvid uppkopplingsmetodiken anpassar sig till efterfrågad typ av datapaket genom att repetitivt fråga åtkomstblockeringen efter tillåten typ av datapaket ända till dess att rätt typ påträffas genom att minnas och repetitivt utelämna felaktiga förfrågningar, och genom, att vid rätt fråga förändra datapakets datastruktur till efterfrågad struktur för den specifika port som står tillbuds för kommunikationen; och

varvid ett externt nätverk upprättas via den externa centrala servern (30) belägen utanför nätverken (10, 12, 14) för samtidig kommunikation genom åtminstone två lagringsmedium (24, 26, 28) och dess programvara, varvid tunnling (32) genom åtkomstblockeringen har åstadkommits utan att göra intrång i nätverket (10, 12, 14) i sig, medförande mot åtkomstblockeringen fri kapacitet för kommunikation med datapaket.

11. Förfarande för nätverksanslutning enligt krav 10, **kännetecknad** av att metodiken anges av följande pseudokod vid uppkoppling mot önskad port:

```
Kolla om proxy skall användas
Om "OK"
 Prova HTTP-proxy
 Om "OK"
  Koppla upp via HTTP-proxy
 Annars
  Prova SOCKS4-proxy
  Om "OK"
   Koppla upp via SOCKS4-proxy
  Annars
   Prova SOCKS5-proxy
   Om "OK"
    Koppla upp via SOCKS5-proxy
   Annars
    Prova direktuppkoppling
    Om "OK"
     Gör direktuppkoppling
    Annars
     Uppkoppling misslyckades eller prova ny port.
Annars
 Prova direktuppkoppling
 Om "OK"
  Gör direktuppkoppling
 Annars
  Uppkoppling misslyckades eller prova ny port.
```

12. Förfarande för en nätverksanslutning enligt krav 10, **kännetecknat** av att metodiken innefattar för framtida generation av proxy/brandväggar (20) som bara släpper igenom

"godkänd" trafik, att detta kringgås genom att gömma skickat data genom att sända över en fejkad HTML-sida med datat maskat.

13. Förfarande för en nätverksanslutning enligt krav 10-12, **kännetecknat** av att filer åtkomstbara via värddatorn (29) hämtas och krypteras i värddatorns temporära katalog, varvid de läggs ut krypterade på den externa centrala servern (30) med bestämd åtkomstprofil som medger åtminstone läsning av filen men inte kopiering från dator utanför nätverket med ansluten värddator (29), vilket medger display av filer utanför nätverket (10, 12, 14).

14. Förfarande för en nätverksanslutning enligt krav 10-13, **kännetecknat** av att mediet (24, 26, 28) medger dess användare att röra sig i ett främmande nätverk (10, 12, 14) och kommunicera externt via den externa centrala servern (30) med andra användare av mediet via tunnlingen (32).

15. Förfarande för en nätverksanslutning enligt krav 10-14, **kännetecknat** av att mediets (24, 26, 28) programvara innefattar IP-telefoni, varvid användare av mediet från valfri datoriserad anordning (16, 29) i valfritt nätverk (10, 12, 14) kan upprätta spontan mobil IP-telefoni via den centrala servern (30).

16. Förfarande för en nätverksanslutning enligt krav 10-15, **kännetecknat** av att skapa åtminstone ett av en radiokanal och filmkanal med andra användare i det externa nätverket genom att mediets (24, 26, 28) programvara innefattar streaming media, varvid användarna kan konsumera musik och film.

17. Förfarande för en nätverksanslutning enligt krav 10-16, **kännetecknat** av att mediets (24, 26, 28) programvara innefattar versionshantering, vilket medför att tidigare versioner av filer kan återskapas genom att spara undan förändringar i ett separat minne i den centrala externa servern (30) som kopplas på/av genom en omkopplare för detsamma på begäran av en användare.

18. Förfarande för en nätverksanslutning enligt krav 10-17, **kännetecknat** av att mediets (24, 26, 28) programvara medger flera användare av detsamma att bearbeta en gemensam textfil i realtid genom den centrala externa servern (30).

Sammandrag

Uppfinningen avser Handhållen nätverksanslutning skapad med åtminstone två lagringsmedium (24, 26, 28) i fickformat, med programvara för kommunikation av datapaket mellan åtminstone två nätverks (10, 12, 14) åtkomstblockering i form av åtminstone ett av en brandvägg (20), SOCKS, IP-filter, eller proxy. Varje lagringsmedium (24, 26, 28) har ett gränssnitt mot en värddator (29) i nätverken (10, 12, 14) och som via programvaran upprättar kommunikation med värddatorn (29) inuti nätverket (10, 12, 14) genom att låna värddatorns (29) temporära kataloger, vilket ger åtkomst till värddatorn (29) utan att störa värddatorns filstruktur. En krypto-daemon enligt uppfinningen innefattar en uppkopplingsmetodik som prövar att upprätta en tunnling (32) genom åtkomstblockeringen mot en central extern server (30) avseende typ av tillåtna datapaket för kommunikation mot existerande typ av åtkomstblockering. Genom uppfinningen upprättas ett externt nätverk via den externa centrala servern (30) belägen utanför nätverken för samtidig kommunikation genom åtminstone två lagringsmedium (24, 26, 28) och dess programvara, varvid tunnling (32) genom åtkomstblockeringen har åstadkommits utan att göra intrång i nätverket (10,12, 14) i sig, medförande mot åtkomstblockeringen fri kapacitet för kommunikation med datapaket. (Fig. 2)

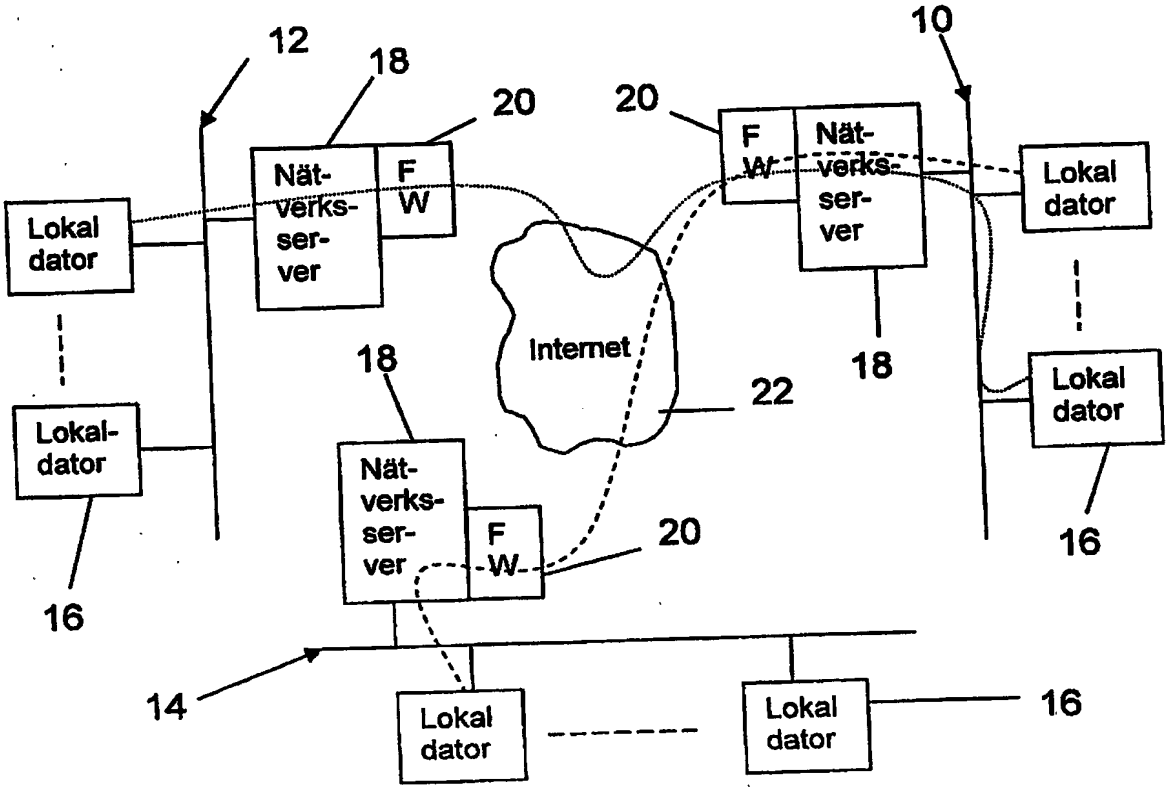

Fig. 1

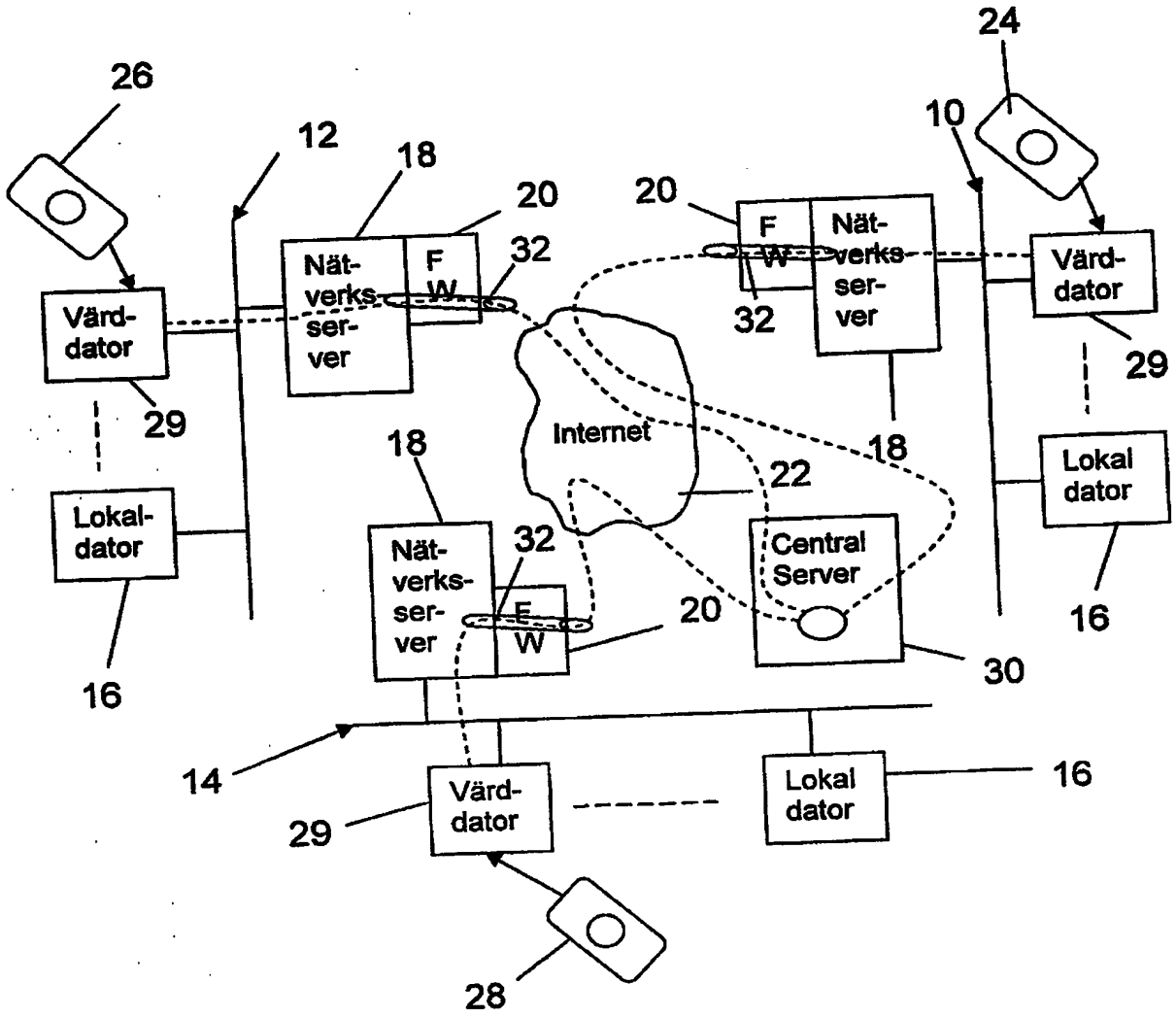
26
12
18
20
32
Värd-dator
Nät-verks-ser-ver
F W
29
Lokal-dator
16
18
Nät-verks-ser-ver
32
F W
20
14
Värd-dator
29
28
Internet
22
Central Server
30
20
32
F W
Nät-verks-ser-ver
18
24
10
Värd-dator
29
Lokal dator
16
Lokal dator
16

Fig. 2